REMARKS

Claims 3, 4, 6, 10, 11, 19 and 20 have been cancelled. New claims 21-41 have been added.

Election of Claims

Applicant hereby confirms the election without traverse to prosecute the invention of Group I, claims 1-12 and 19. In so doing, Applicant reserves the right to pursue the invention of Group II in a divisional application at a later date. Because Applicant has seen fit to substantially amend claim 19, the original claim 19 has been cancelled but has been reintroduced with more limitations as new claim 24. New claim 24 is also directed toward a certificate library (as was claim 19) and includes many of the limitations of original claim 19. Thus Applicant respectfully submits that new claim 24 (and its dependent claims 25-28) be examined in Group I. New claims 21-23 that depend from claim 1 have been added and it is requested that these claims also be examined along with claim 1.

New claims 29-33 have been added that are directed to a certificate store system for creating a digital certificate. As the claims of elected Group I are also directed to creating or storing digital certificates, Applicant respectfully requests that new claims 29-33 also be examined along with the claims of Group I.

Applicant understands that claims 13-18 have been withdrawn from consideration, but respectfully requests that the amendments to these claims be entered to place the claims in better form for a divisional application. New claims 34-36 have also been added that depend from claim 13. New claims 37-41 have been added that are directed to a chip card for authentication; it is submitted that these claims be entered to place the claims in better form for a divisional application.

Objections to the Drawings

Formal drawings are being submitted herewith. The drawings have also been objected to because the steps of accessing the digital certificate using the issuing-party identifier or the merchant-specific identifier of claims 5 and 6 are not shown. Claim 6 has been cancelled and its objection is now moot.

Regarding claim 5, Applicant points out that Figure 4A at step 412 shows "RELIANT PARTY MAKES REQUEST TO CERTIFICATE LIBRARY AND GETS RESPONSE." Applicant submits that this step of Figure 4A (which inherently includes its supporting disclosure in the specification), does show "accessing the digital certificate using the issuing-party identifier." For example, the specification at page 19, line 4 through page 19, line 19 describes step 412. Lines 8-12 of page 19 specifically point out that the reliant party requests whether the user has a digital certificate issued by the reliant party using the memory location and LDAP parameters. One of skill in the art will readily realize that a memory location or a parameter can serve as an identifier. In this specific situation, the reliant party is the issuer, so any memory location or parameter that identifies the reliant party would be an "issuing-party identifier." Thus, Applicant submits that step 412 of Figure 4A does show the features of claim 5.

Further, the specification discloses elsewhere this feature of claim 5. For example, page 4 at lines 20-22 discloses that the digital certificate is identified by a unique identifier of the reliant party. Page 5 at lines 3-5 discloses that the entity provides parameters to identify a particular certificate needed by the entity. Page 10 at lines 10-12 disclose that a merchant uses parameters, such as an appropriate certificate identifier, to access a digital certificate chain. Page 15, lines 23-26 disclose that a merchant can access a memory location to determine if there is a digital certificate issued by that merchant or recognizable to the merchant. Page 17 at line 22 discloses a specific address that can serve to identify a "Member Bank" as the issuer of a digital certificate.

Although Applicant believes that the feature of claim 5 is shown in the figures, Applicant is willing to amend one or more of the drawings (based on the above disclosure) if the Examiner so insists.

Regarding reference character "202" in Figures 2 and 3, a corrected drawing Figure 2 is submitted that refers to a "Certificate Library Directory" instead of a "Certificate Library." Thus "202" identifies "Certificate Library Directory" in the figures.

Objections to the Specification

As per the Examiner's suggestion, the title of the application has been changed to be more descriptive. Regarding the objections detailed in paragraph 9 of the Office Action, Applicant submits that the above amendments to certain paragraphs of the specification address all of the Examiner's concerns.

Objections to the Claims

Claims 3, 4 and 6 have been cancelled and it is submitted that their objections are now moot. Claims 1 and 2 have been amended to remove the indefinite language; it is submitted that claims 1 and 2 as they now read are definite.

The Present Invention

As pointed out in the Background of the present application, the memory on chip cards can be limited. The present invention provides a way for any number of digital certificates (or certificate chains) for a user to be stored on a remote certificate library server (along with the user's public key), while the user's private key is safely stored on the user's chip card. When the chip card is used, an address on the chip card provides the location of the certificate library server where the user's certificates are stored. An entity can also access the user's chip card to provide authentication using the stored private key.

Rejection of the Claims

Claim 1

Claim 1 has been rejected as being unpatentable over *Stallings* Cryptography and Network Security ("*Stallings*") and VeriSign Certification Practice Statement. *Stallings* discusses use of the X.509 digital certificate format, but does not disclose a user private key being stored on the user's chip card. Nor does *Stallings* disclose that an address of the certificate library is also stored on the chip card, thus allowing an entity accessing the chip card to easily access the library where the user's digital certificate is stored. Claim 1 specifically requires "storing said user private key and an address of said certificate library server on a chip card of said user." The advantage of the invention of claim 1 is that the chip card need only store the private key and a library address; the much larger digital certificate can be stored remotely on a certificate library server.

Claim 9 requires a challenge and response protocol using the private key stored on the user's chip card. The advantage is that the private key can authenticate the chip card (and to a certain extent the user) to an outside party.

Claim 19 (reintroduced as new Claim 24)

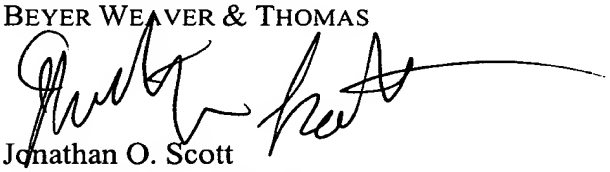
New claim 24 requires "a user first cryptographic key included in each of said digital certificate chains, said user first cryptographic key having a corresponding user second cryptographic key being stored in the chip card of said user." *Stallings* and the cited art do not disclose that a first user key stored in the certificate library server has a corresponding second user key stored in a chip card. As pointed out in the specification of the present application, these first and second user keys can be symmetric keys or asymmetric keys.

New Claim 29

As mentioned above, new claim 29 is directed to a system that creates a digital certificate, thus it is submitted that it should be examined along with the other claims of Group I. Claim 29 requires "a chip card that stores said user second cryptographic key, an address of said certificate library server, an identifier of said registration authority, and a software application that coordinates communication between said chip card and said certificate library server." It is respectfully submitted that *Stallings* and the other art of record do not disclose a chip card that stores a user cryptographic key (where the corresponding other key is stored in a remote digital certificate), an address of a certificate library server, and a software application that coordinates communication between the chip card and the library server.

Reconsideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS



Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778

Telephone: (612) 252-3330
Facsimile: (612) 825-6304